SHUMAKER & SIEFFERT, P.A.
8425 SEASONS PARKWAY, SUITE 105
ST. PAUL, MINNESOTA 55125
TEL 651.735-1100
FAX 651.735-1102
WWW.SSIPLAW.COM

FACSIMILE SUBMISSION UNDER 37 CFR 1.8

TO: Examiner Aravind K. Moorthy	FROM: Kent J. Sieffert
COMPANY: USPTO – Mail Stop AF	DATE: NOVEMBER 7, 2006
FAX NUMBER: 571-273-8300	TOTAL NO. OF PAGES INCLUDING COVER: 8
PHONE NUMBER:	SENDER'S REFERENCE NUMBER: 1014-056US01 / JNP-0251
RE: Notice of Appeal/Pre-Appeal Brief Request for Review in Response to FOA dated 8-7-06	APPLICATION SERIAL NUMBER: 09/900,515

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Michael Freed; Elango Ganesan; Praveen Patnala	Confirmation No.	4141
Serial No.:	09/900,515		
Filed:	July 6, 2001	Customer No.:	28863
Examiner:	Aravind K. Moorthy		
Group Art Unit:	2131		
Docket No.:	1014-056US01/ JNP-0251		
Title:	SECURE SOCKETS LAYER CUT THROUGH ARCHITECTURE		

CERTIFICATE UNDER 37 CFR 1.8 I hereby certify that this correspondence is being transmitted via facsimile to the United States Patent and Trademark Office on November 7, 2006.

By: Caryl Harriman
Name: Caryl Harriman

MAIL STOP AF
Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

We are transmitting herewith the attached correspondence relating to this application:

☒ Transmittal sheet containing Certificate of Mailing
☒ Notice of Appeal (1 pg.)
☒ Pre-Appeal Brief Request for Review (5 pgs.)

Please apply any charges not covered, or any credits, to Deposit Account No. 50-1778.

Date:
November 7, 2006

By: Kent J. Sieffert
Name: Kent J. Sieffert
Reg. No.: 41,312

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Michael Freed; Elango Ganesan; Praveen Patnala	Confirmation No.	4141
Serial No.:	09/900,515	Filed:	July 6, 2001
Examiner:	Aravind K. Moorthy	Group Art Unit:	2131
Docket No.:	1014-056US01/JNP-0251	Customer No.:	28863
Title:	SECURE SOCKETS LAYER CUT THROUGH ARCHITECTURE		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

In the Office Action, the Examiner rejected claims 1-8, 11, 45-47, 51 and 53 under 35 U.S.C. 102(e) as being anticipated by Ellis (USPN 6,484,257). The Examiner rejected claims 9, 10, 12-44, 48-50 and 52 under 35 U.S.C. 103(a) as being unpatentable over Ellis in various combinations with other references. This rejection is improper. Applicant requests formal review of the factual basis set forth by the Examiner.

Applicants' claim 1 is directed to a method and requires managing a communications negotiation between the client and the server through an intermediate device that supports both a direct mode and a proxy mode. Claim 1 requires decrypting encrypted data packets with the intermediate device. Claim 1 then makes a distinction as to how the unencrypted data packets are forwarded by the intermediate device based on whether the intermediate device is operating in direct mode or proxy mode.

Specifically, clam 1 requires forwarding unencrypted data packets from the intermediate device to the server *using a communication session negotiated by the client and the server* when the intermediate device operates in *direct mode*. Claim 1 further requires forwarding unencrypted data packets from the intermediate device to the server *using a second communication session negotiated by the server and the intermediate device* when the intermediate device operates in proxy mode. That is, depending on the mode, the Applicants' claimed intermediate device decrypts data packets and either transparently uses the same communication session negotiated by a client and a server to forward the decrypted data to the server (direct mode) or uses a separate session negotiated by the intermediate device and the server (proxy mode).

In rejecting claim 1, the Examiner asserts that Ellis describes an intermediate device that supports both a direct mode and a proxy mode as defined by Applicants' claims.[1] As a basis for this assertion, the Examiner cites Ellis at col. 7, ln. 11 – col. 8. ln. 27. The Examiner clarified his position on page 2 of the Final Office Action as follows:

> *Ellis discloses a direct mode. The direct mode as taught by Ellis is when the clients are communicating directly without interference of the 'main server". The proxy mode is when communication goes through the main server.*

This statement is very revealing as to the Examiner's factual error.

First, as made clear by this statement, the Examiner asserts that the Ellis system includes an intermediate device (the "main server") that operates in a "direct mode" when the clients communicate directly "without interference" from the main server. The Examiner then distinguishes this from proxy mode where "communication goes through the main server."

This, however, overlooks the fundamental requirements of Applicant's claim 1 that in **both** modes the intermediate device decrypts the encrypted data packets and forwards the decrypted data packets. For example, claim 1 specifically requires forwarding **unencrypted** data packets **from the intermediate device** to the server *using a communication session negotiated by the client and the server* when the intermediate device operates in *direct mode*. In other words, claim 1 requires that the intermediate device that decrypted the data packets forward the **decrypted** data packets to the server using a session that the client and server negotiated when operating in direct mode. In this manner, the direct mode allows the intermediate device to transparently receive encrypted data packets, decrypt the data packets and then forward the decrypted data packets to the server using the session that the client and server negotiated. In contrast, in proxy mode, the intermediate device that decrypted the data packets use a separate session that was "negotiated by the server and the intermediate device."

The Examiner's assertion that Ellis describes an intermediate device that supports a "direct mode" because the clients effectively bypass the intermediate device (i.e., the main server) and communicate directly without the communications going through the intermediate device overlooks these basic claim requirements. None of the components of the Ellis system

[1] Office Action, pg. 2.

operates as an intermediate device that supports both a direct mode and a proxy mode as defined by Applicants' claims.

The Examiner elaborated on page 3 of the Final Office Action with respect to the "direct mode" taught by Ellis by stating:

> *Applicant argues that [Ellis fails to teach that] the intermediate device operates in a direct mode to decrypt data encrypted data packets and forward unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server.*
>
> *The examiner disagrees. Ellis discloses forming a session between a client and the agent server. The agent server decrypts the session communication and redirects the decrypted data to its final destination.*

The error of this logic should be apparent on its face. Applicant's claim requires that, in direct mode, the intermediate device decrypts data encrypted data packets and forward unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server (i.e., not the intermediate device). To the contrary, the plain language of the Examiner's argument is that the "agent server decrypts the session communication [apparently as an intermediate device]" and redirect the decrypted data using a session between a client and that same agent server. This, therefore, would not teach or suggest a direct mode in which an intermediate device utilizes a session that it did not negotiate, i.e., a session that the client and the server negotiated, to forward decrypted data packets to that server, as required by claim 1.

As explained in Applicant's previous responses, Ellis describes a distributed computing environment having a main server, agent servers and clients. Both the main server and the agent servers are enabled to receive secure connections.[2] Ellis describes two general scenarios: (1) handling new connections, and (2) redirecting existing connections. With respect to a client request for a new connection, the agent server and the client then negotiate the new session.[3] The agent server then receives encrypted session communications from the client via the negotiated session, decrypts the session communication and forwards the decrypted data to its

[2] Ellis at col. 7, ln. 22.

[3] Ellis makes it abundantly clear that the client and the agent server negotiate the session. Ellis at col. 7, ln 54, for example, states that the client and the agent "independently generate" session keys for new session. At col. 8, ln. 46, Ellis describes 6 steps of an "overall system algorithm." In Step 5, Ellis states that the client and the agent server "negotiate" the session key and the proper security association. Ellis then illustrates each packet having an AGENT IP HEADER 5A24, which is a clear indication that the session is between the client and the Agent.

proper destination. Thus, as admitted by the Examiner, with respect to new sessions, the client and the agent server are responsible for negotiating the new session. Thus, with respect to new connections, the main server and the agent servers in Ellis appear to be operating as the classical proxy servers on behalf of destinations, and the main server (as an intermediate device) certainly does not use sessions negotiated by the client and the destination for forwarding decrypted data.

With respect to the second scenario, i.e., redirecting existing connections, Ellis states that the main server may "pass" an existing session from one agent server to another different agent server.[4] If an agent server becomes saturated, for example, it notifies the main server to "pass the session on to another agent server."[5] During this process, the main server notifies the client, and the client connects to the new agent server.[6] The new agent server uses security information for the session to continue the secure session with the client. That is, the new agent server has replaced the role of the original agent server. The previous agent server then closes the original session.[7]

In this regard, it is reasonably clear that the new agent server replaces the role of the previous agent server as operating as an end-point for a session with the client. Therefore, even for redirected existing sessions, the new agent server again operates as a proxy server by receiving encrypted communications from the client via a session negotiated by the agent server and that client, decrypting the communications, and then forwarding the decrypted communications to the ultimate destination.

For at least these reasons, Ellis fails to teach or suggest an intermediate device that supports both a direct mode and a proxy mode. There is no teaching or suggestion in Ellis of an intermediate device located between a client and a server, where the intermediate device operates in a direct mode to decrypt encrypted data packets and forward unencrypted data packets from the intermediate device to the server using a communication session *negotiated by the client and the server*. In contrast, the intermediate devices (agent servers) of Ellis only operate as proxies that separately negotiate communication sessions with clients on behalf of destinations.

For at least these reasons, Ellis fails to anticipate the requirements of independent claims 1, 33 and 45. Moreover, none of the other references, either singularly or in combination, provide any teaching or suggestion that overcomes the deficiencies of Ellis.

[4] Ellis at col. 8, ln. 8.
[5] Ellis at col. 8, ll. 8-9.
[6] Ellis at col. 8, ll. 14-15.
[7] Ellis at col. 8, ll. 21-22.

With respect to dependent claim 3, nothing in Ellis suggests modifying a SYN request. In fact, in its entirety, Ellis does not even refer to a SYN request, let alone modification of a SYN request by an intermediate device. On this point, the Examiner stated that in Ellis the SYN request is modified by the "decryption of the requests." This is factually incorrect. SYN requests are used to establish sessions and encryption / decryption of data cannot occur until after a session is established, i.e., after the TCP handshake.

With respect to dependent claims 51 and 53, the Examiner asserted that Ellis teaches *automatically switching* the intermediate device from the direct mode to the proxy mode upon detecting a communication error associated with the direct mode. In rejecting claims 51 and 53, the Examiner again cited Ellis at col. 7, ln. 11 to col. 8, ln. 27 without comment. Applicants are at a loss as to where the Examiner finds a teaching for an intermediate device that *automatically switches* from the direct acceleration mode to the proxy mode upon detecting a *communication error* associated with the direct mode.

Please charge any additional fees or credit any overpayment to deposit account number 50-1778.

Date:
November 7, 2006

By:

Name: Kent J. Sieffert
Reg. No.: 41,312

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102